9. *Сафронов А.И., Горковец А.С., Ермакова А.Е.* Анализ отечественного и зарубежного опыта обеспечения информационной безопасности с целью определения направлений развития интеллектуальных транспортных систем на городской электричке / Интеллектуальные транспортные системы IV. – М.: РУТ, 2025. – С. 717-725.

10. *Котов В.Е.* Сети Петри. – М.: Наука, 1984. – 160 с.

11. *Сафронов А.И.* Применение дополненного аппарата сетей Петри для моделирования процесса автоматизированного построения плановых графиков движения пассажирских поездов метрополитена / Проблемы управления безопасностью сложных систем XXXII. – М.: ИПУ РАН, 2024. – С. 433-439.

Клименко Ю.А., Преображенский А.П., Тихонов И.А.

Моделирование системы безопасности умного дома

Аннотация: В работе представлена модель умного дома, на основе которой можно дать оценку его степени защищенности. Представлены численные значения показателя риска нарушения конфиденциальности информации. Приведен типовой сценарий функционирования системы.

Ключевые слова: умный дом, защищенность, риск, система, модель

В настоящее время «Умный дом» можно рассматривать в виде весьма востребованных и широко распространенных примеров внедрения IoT-решений. внутри него объединяются разнообразные устройства в единую сеть, которая управляется удаленно с использованием интернет-соединения [1]. При этом данные в системе могут быть привлекательными целями для киберпреступников. Устройства, входящие в систему «Умного дома», могут собирать и хранить чувствительную информацию, такую как аудио-, видеоданные, координаты местоположения и

поведенческие шаблоны пользователей, что создает серьезные риски нарушения конфиденциальности.

Цель данной работы – разработка алгоритма оценки рисков в системе умного дома для повышения уровня его защищенности.

Построение модели базируется на методологиях STRIDE [2] и PRASH [3]. Они дополняются описанием компонентов системы, политики конфиденциальности, а также классификацией типов обрабатываемых данных.

Модель представляется в виде шестикомпонентной структуры S = (H, N, U, L, D, P). При этом каждая из компонент относится к некоторому действию:

– H (Дом) – пользователи физическим образом находятся в доме. При этом могут быть выделены жилые зоны (в качестве примера, можно указать комнаты). Тогда формируется множество $H = \{z_1, z_2, ..., z_n\}$, при этом $z_i \in LC$ соответствует некоторой жилой зоне.

– N (Устройства) – совокупность компонентов, которые интегрированы в инфраструктуру «Умного дома». Справедливо выражение: $N = C \cup M \cup B$, где C – пользовательские устройства; M – пользовательские терминалы; B – устройства для того, чтобы вести обработку данных.

Внутри умного дома характеристики устройств задаются на базе множества CP (capabilities). Справедливо отношение $I \subseteq N \times CP$. Учитывается, что реализация возможности CP узлом n задается выражением I (n, cp). Зоны внутри дома и устройства связаны на основе выражения: $fnl: N \rightarrow LC$.

– U (Пользователи) рассматриваются в виде субъектов, для которых с системой взаимодействие происходит или на основе приложений или напрямую. Если проводить анализ пользователей, то представляет интерес множеств R = {субъект данных, контроллер данных, пользователь данных}. Кроме того, есть отношение $At \subseteq U \times R \times N$. Оно дает возможность для связи пользователя и некоторого устройства: тогда At (u, r, n) показывает, что будет взаимодействие с ролью r пользователя u и некоторого узла n.

– L (Каналы) могут считаться соединениями. На их базе будет обмен данными между узлами и пользователями: $L \subseteq (N \times N) \cup (N \times U) \cup (U \times N)$, описывающий возможные направления передачи информации.

– D (Информация) считается совокупностью данных, которые в системе подвергаются обработке. Каждая единица представляется кортежем s = (di, ds, dp, dt, dl, de), где:

di – сами данные, которые фиксируются устройствами;

ds – субъект, к которому относятся данные (пользователь или система);

dp – цель обработки информации (например, идентификация пользователя);

dt – срок хранения данных: {неопределенно, до достижения цели, до установленной даты};

dl – признак явной идентификации, указывающий, можно ли напрямую определить ds по di (например, по голосу или MAC-адресу);

de – меры по защите конфиденциальности: управление ∈ {анонимизация, деидентификация, шифрование}, фаза ∈ {генерация, сбор, обработка, раскрытие} – этап жизненного цикла данных, к которому применяется метод защиты.

Разработанная формальная модель, предназначена для выявления уязвимостей конечных устройств и каналов передачи данных.

Исходя из общепринятой методики оценки рисков в сфере компьютерной безопасности, риск нарушения конфиденциальности информации – это комбинация оценки возникновения нарушения конфиденциальности информации и последствий (ущерб). Необходимо совместным образом рассматривать как вероятность реализации атаки, так и возможные последствия от ее успешного проведения. Такой подход соответствует принципу, закрепленному в международных стандартах, в частности:

– ISO/IEC 27005, где риск определяется как функция от вероятности наступления события и величины ущерба;

– FAIR (Factor Analysisof Information Risk), где риск трактуется как произведение частоты события и масштабов потерь;

– Методикам PRASH и EPIC, применяемым для оценки рисков в интеллектуальных системах и средах интернета вещей.

Описывается мера риска следующим уравнением (4) и имеет численные значения (таблица 1)

$$r_{\mu} = \alpha_{l.} \times \alpha_{i} \qquad (1)$$

Рассмотрим типовой сценарий функционирования системы. Камера видеонаблюдения у входа в дом (Ring Video Doorbell) фиксирует появление посетителя (r1), активирует сенсоры движения, микрофон и видеозапись. Полученные данные передаются через защищенный канал на мобильное устройство пользователя (Mobile Device), обеспечивая мгновенное уведомление о событии (r2). В ответ пользователь отдает голосовую команду с помощью голосового помощника Amazon Echo (r3), которая обрабатывается локальным образом и пересылается в облачную систему (Cloud) (r4) для верификации и принятия решения о доступе. После успешной обработки команда направляется на электронный замок AugustSmartLock (r5), который открывает дверь при подтверждении аутентичности запроса.

Таблица 1 – Численные значения показателя риска нарушения конфиденциальности информации

Численная оценка	Описание
6,0 – 12,0	Уязвимость легко эксплуатируется и может привести к серьезному нарушению конфиденциальности данных
3,0 – 5,9	Уязвимость требует определенных условий для эксплуатации, но все же представляет угрозу для конфиденциальности пользователя
0,1 – 2,9	Для реализации атаки необходимы значительные ресурсы или специализированные знания; потенциальный ущерб для конфиденциальности – незначителен
0	Отсутствуют условия для эксплуатации уязвимости; риск нарушения конфиденциальности отсутствует

Так, устройство FacebookPortal, подключенное через Wi-Fi и Bluetooth, может использоваться для отображения входящих уведомлений, видеозвонков или медиа, а также предоставлять интерфейс для взаимодействия с Alexa. При этом уязвимость в веб-браузере устройства позволяет считывать историю посещений и личные данные, представляя угрозу конфиденциальности. AmazonEcho, функционирующий по Bluetooth и Wi-Fi, подвержен уязвимости, которая позволяет злоумышленнику получить доступ к

памяти процесса через стек Bluetooth, что представляет риск раскрытия личной информации.

Камера TuyaSmartCamera, подключенная через Wi-Fi и взаимодействующая с облачной платформой, также может быть целью атак. Уязвимость создает риск отказа в обслуживании, что может нарушить видеомониторинг. Устройство SylvaniaSmartHome, взаимодействующее с мобильным приложением через Wi-Fi и Zigbee, уязвимо из-за неправильного контроля доступа в мобильном APK-файле что может привести к компрометации паролей и персональных данных. Центральным связующим элементом в сети зачастую выступает маршрутизатор Tenda AC6, на который приходится основная нагрузка по маршрутизации трафика. Уязвимость делает возможным вмешательство в передаваемые данные, включая подмену или перехват команд и конфиденциальной информации.

В таблице 2 приведены значения рисков для разных компонентов системы.

Таблица 2 – Оценка рисков по компонентам системы

Устройство / Уязвимость	Значение риска	Уровень риска
FacebookPortal / CVE-2018-6177	2.88	Низкий
AmazonEcho / CVE-2017-1000250	4.05	Средний
RingDoorbell / CVE-2019-9483	7.8	Высокий
AugustSmartLock / CVE-2019-17098	5.07	Средний
TuyaSmartCam / CVE-2024-32268	1.08	Низкий
SylvaniaHome / CVE-2024-48544	1.35	Низкий
Tenda AC6 Router / CVE-2024-46450	10.8	Высокий

Вывод

Проведенный анализ показал, что система «Умный дом» представляет собой сложную архитектуру, в которой множество устройств обмениваются информацией через локальные и облачные каналы связи. На каждом этапе передачи присутствуют потенциальные угрозы, связанные с уязвимостями программного обеспечения и аппаратных компонентов. Далее для каждого из перечисленных устройств была проведена оценка рисков на основе изучения открытых баз данных уязвимостей (CVE, NVD), научных

публикаций и результатов тестирования с использованием методик CVSS 3.0.

Литература:

1. *Sarkar Hasan Ahmed, Subhi R.M. Zeebaree*. A survey on Security and Privacy Challenges in Smarthome based IoT // International Journal of Contemporary Ar-chitecture "The New ARCH". – 2021. – Vol. 8, No. 2. – P. 489-510.

2. *Alrawi O., Lever C., Antonakakis M., Monrose F.* Sok: Security evaluation of home-based iot deployments / Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP). – San Francisco, CA, USA, 2019. – P. 1362-1380.

3. *Kenneally E.* Privacy and Security // IEEE Internet of Things Magazine. – 2018. – Volume 1. Issue 1. – P. 8-10.

4. *Вольвач А.В., Поддубная Н.С.* Уязвимости системы «Умный дом» // Московский государственный технический университет гражданской авиации. – 2021. – Вып.1 (52). – С. 49-52.

5. *Воевода А.А., Романников Д.О.* Синтез нейронной сети для решения логико-арифметических задач // Труды СПИИРАН. – 2017. – Вып. 5 (54). – С. 205-223.

6. *Min Li, Wenbin Gub, Wei Chenc, Yeshen Hed, Yannian Wud, Yiying Zhange.* Smart home: Architecture, Technologies and Systems. 8th International Congress of Information and Communication Technology (ICICT-2018) // Procedia Computer Science. – 2018. – Vol. 131. – P. 393-400.

7. *Kandasamy K., Srinivas, S., Achuthan, K., Rangan V.P.* IoT cyber risk: A holis-tic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process // EURASIP J. Inf. Secur. – 2020. – P. 1-18.

8. *Ланкин Ю.П., Басканова Т.Ф., Лобова Т.И.* Нейросетевой анализ сложноорганизованных экологических данных // Современные проблемы науки и образования. – 2012. – № 4. – URL: https://www.science-education.ru/ru/article/view?id=6754 (дата обращения 12.09.2025).

9. *Klimenko Yu.A., Preobrazhensky A.P.* Development of a passive system for determining the positioning of an unmanned aerial vehicle // Modern problems of radio electronics and telecommunications, founders: Sevastopol State University. – 2024. – №7. – P. 33.

10. *Клименко Ю.А., Львович Я.Е., Преображенский А.П.* Проектирование контрольно-измерительных компонент распределительных энергетических систем // Advanced Engineering Research (Rostov-on-Don). – 2024. – Т. 24. № 1. – С. 88-97.

Хабибулин Р.Ш.

Имитационная модель оперативных фаз реагирования на пожары объектов топливно-энергетического комплекса с робастной оптимизацией времени, риска и ресурсов

Аннотация: В работе представлена имитационная модель управления оперативными фазами реагирования пожарно-спасательных подразделений на пожары объектов топливно-энергетического комплекса (ТЭК). Модель основана на статистическом анализе эмпирических данных 195 пожаров на нефтебазах и нефтехранилищах, зарегистрированных в период с 2009 по 2021 год. Разработан методологический подход робастной многокритериальной оптимизации, учитывающий три ключевых критерия управления: время выполнения оперативных фаз, уровень риска неблагоприятных условий и объем затрачиваемых ресурсов.

Ключевые слова: оперативные фазы реагирования, пожарная безопасность, топливно-энергетический комплекс, имитационное моделирование, робастная оптимизация, метод Монте-Карло

Введение

Оперативное реагирование пожарно-спасательных подразделений на пожары объектов топливно-энергетического комплекса (далее – ТЭК) представляет собой сложный стохастический процесс, характеризующийся высокой степенью неопределенности [1, 2]. Объекты ТЭК, включающие нефтебазы, нефтехранилища и резервуарные парки, относятся к категории опасных производственных объектов первого класса опасности, где последствия пожаров могут иметь катастрофический характер.